

REMARKS

In accordance with the foregoing, the specification and claims 1 and 6 have been amended. Claim 2 has been cancelled without prejudice or disclaimer. Claims 1 and 3-6 are pending and under consideration.

REJECTIONS UNDER 35 U.S.C. §§102 AND 103:

Claims 1 and 4-6 are rejected under 35 U.S.C. §102(b) as being anticipated by Van Oorschot et al. (U.S. Patent No. 5,669,431). Claims 2 and 3 are rejected under 35 U.S.C. §103(a) as being unpatentable over Van Oorschot et al. in view of Micali (U.S. Patent No. 5,717,758) in further view of Micali (U.S. Patent No. 6,487,658, Micali II).

Amendments are now made to claims 1 and 6 in order to clearly describe characteristics of the present invention without adding new matter because the claims are amended and new claims are added based on content in the specification, page 8 lines 4 to 19.

The present invention as claimed is distinguishable from the cited references Van (5,699,431), Micali (5,717,758) and Micali II (6,487,658) based on the following arguments.

At first, the present invention as claimed defines the hash function H() and calculates a result of the hash function H() by inputting value S which is the subject name (SUBJECT_NAME) in the certificate.

In Van, there is no description of calculating the result of the has function by inputting the value S.

Secondly, the present invention as claimed defines the number of nodes based on the number of expected subscribers in order to prevent concentration of the accesses to a certain CRL node. After defining the number of nodes, the method as claimed distributes the CRL information among the defined number of N nodes in balance.

The above mentioned defining of the number of nodes is not disclosed or taught from Van, Micali and Micali II.

Finally, the present invention calculates the distribution interval by using equations $H(s) = V$ and $\frac{V_{\max} - V_{\min}}{N} = I$. That is, a plurality of V is calculated by inputting the subject name to the

hash function $H(S)$. Among the plurality of V , the maximum value V_{\max} and minimum value V_{\min} are selected and the distribution interval is calculated by dividing the difference between V_{\max} and minimum value V_{\min} by the number nodes N .

The above mentioned calculating method is not disclosed and taught by Van, Micali and Micali II.

As mentioned above, the present invention is distinguishable from cited references Van, Micali and Micali II and, therefore, the pending claims of the present invention are patentable.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: _____

9/9/04

By: _____



Michael D. Stein
Registration No. 37,240

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501